

⑫

DEMANDE DE BREVET EUROPEEN

② Numéro de dépôt: 87401435.0

Int. Cl.4: **G 06 F 12/14**

②② Date de dépôt: 23.06.87

(30) Priorité: 27.06.86 FR 8609358

④3 Date de publication de la demande:
03.02.88 Bulletin 88/05

84) Etats contractants désignés:
DE ES FR GB IT NL

⑦ Demandeur: THOMSON SEMICONDUCTEURS
101, bld Murat
F-75016 - Paris (FR)

(72) Inventeur: Fruhauf, Serge
THOMSON-CSF SCPI 19, avenue de Messine
F-75008 Paris (FR)

⑦ Mandataire: Guérin, Michel et al
THOMSON-CSF SCPI 19, avenue de Messine
F-75008 Paris (FR)

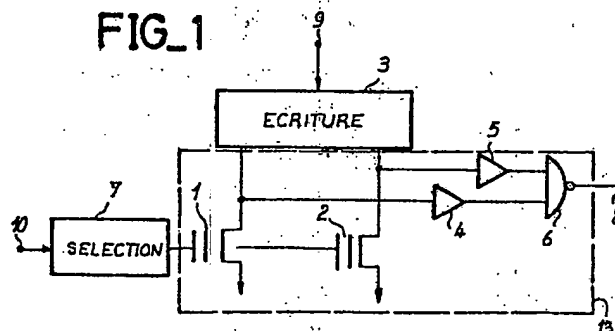
Le titre de l'invention a été modifié (Directives relatives à l'examen pratiqué à l'OEB, A-III, 7.3)

(54) Circuit Intégré de protection à mémoire comprenant deux régions d'adresses sélectionnables.

(67) L'invention concerne un procédé et un circuit de protection de données informatiques.

Deux cellules 1, 2 sont réservées pour prévoir la sélection d'un mode de fonctionnement. Chaque mode de fonctionnement implique une région particulière de la mémoire de données, les régions correspondant aux modes non sélectionnés étant innaccessibles.

FIG_1



Description

PROCEDE DE GESTION D'UN CIRCUIT ELECTRONIQUE ET CIRCUIT METTANT EN OEUVRE UN TEL PROCEDE

La présente invention concerne un procédé de gestion d'un circuit électronique. Elle concerne aussi un circuit mettant en oeuvre un tel procédé. Elle trouve application dans le domaine de la protection matérielle (hardware) des logiciels et des données informatiques.

Dans un nombre croissant d'applications, le fabricant d'un circuit ou l'utilisateur primaire d'un tel circuit subit un risque de copiage des informations, programmes ou données, qu'il inscrit dans une mémoire du circuit. C'est le cas dans le domaine des ordinateurs à logiciels intégrés (moniteurs, systèmes d'exploitations, utilitaires) et aussi dans celui de la carte bancaire. Un moyen consiste à prévoir toutes les procédures d'accès matériel et à prévenir toute tentative non désirée par exemple par destruction de données. Selon un autre moyen, il s'agit de coder les données ou leur séquence de telle manière que l'information qu'elles contiennent devienne inexploitable telle quelle.

Malheureusement, l'ingéniosité des pirates, malgré la qualité des protections contraint le propriétaire à varier autant que possible les modes de protection physique. L'invention propose un moyen particulièrement avantageux. En effet, elle concerne un procédé de gestion d'un circuit électronique comme un circuit à mémoire de mots binaires qui consiste à sélectionner l'un parmi au moins deux modes de fonctionnement du circuit en programmant au moins une cellule de la mémoire, chaque mode impliquant une région d'adresses particulières de la mémoire.

L'invention concerne aussi un circuit électronique comportant une mémoire à cellules de mots binaires caractérisé en ce qu'il comporte deux cellules programmées en parallèle, qui possèdent un unique chemin d'écriture et deux chemins de lecture connectés à un organe de gestion de mode de fonctionnement dont le contenu permet de sélectionner un mode particulier du fonctionnement du circuit, impliquant une région d'adresses particulières de la mémoire.

D'autres caractéristiques et avantages de la présente invention apparaîtront à l'aide de la description d'un exemple non limitatif de réalisation et des figures qui sont :

- la figure 1 : un schéma d'une cellule selon l'invention entourée de ses aides,
- la figure 2 : un schéma d'un circuit complet selon l'invention,
- la figure 3 : un chronogramme d'état de deux bus du circuit,
- la figure 4 : un schéma d'un motif de cellules de mémoire.

On a représenté à la figure 1 un circuit de gestion. Ce circuit comprend une cellule ou préférentiellement deux cellules d'une mémoire EPROM ce qui permet d'établir une redondance dans l'information de sélection. Chaque cellule est ici constituée par un seul transistor à grille isolée d'une mémoire de type EPROM. Les grilles des cellules 1 et 2 sont reliées à

un organe de sélection 7 qui décode l'adresse reçue par la connexion 10. Le chemin d'écriture comporte un registre d'écriture 3 dont chacune des deux sorties est reliée à l'entrée de la cellule 1 ou 2 correspondante. L'entrée 9 du registre reçoit la donnée à inscrire a priori d'un organe de programmation extérieur au circuit à la disposition du légitime propriétaire de l'information. Cette disposition permet entre autres de combiner l'invention, dans un but de sécurité accrue à des techniques de codage ou d'encryptage.

Chaque cellule comporte un chemin de lecture à un amplificateur de lecture 4 ou 5, classique pour toute cellule du plan mémoire. Les sorties des amplis sont connectées à un noeud constitué dans un exemple de réalisation par un circuit de logique combinatoire. Celui-ci comporte dans un mode de réalisation une porte NON ET 6 dont la sortie 8 est connectée à un organe de décodage des adresses de la mémoire utile.

Ainsi, dans le procédé de l'invention, un mode de fonctionnement implique une région d'adresses particulières de la mémoire. Chaque région peut être une succession d'adresses successives. Les régions peuvent être disjointes deux à deux. Le but de l'invention dans tous les cas est d'interdire l'accès à une région d'adresses ne correspondant pas au mode de fonctionnement programmé des cellules 1 et 2, c'est-à-dire sélectionné par le fabricant du circuit de l'invention quand il enregistre les cellules 1 et 2.

Dans un mode de réalisation, la mémoire est du type EPROM de 8 kilo-octets d'adresse. Deux modes de fonctionnement seulement sont prévus. Les deux régions d'adresses correspondantes sont non disjointes. La première région comporte les 4 kilo-octets d'adresses du début de la mémoire et la seconde région comporte 8 kilo-octets complets de la mémoire.

A la figure 2, on a représenté un circuit selon l'invention. Un décodeur 15 reçoit du circuit de gestion 13 qui correspond à un circuit de protection pour la mémoire, un signal 14 lui indiquant quelle région d'adresses 18 ou 19 il peut atteindre dans la mémoire 20 du type EPROM, ce décodeur reçoit également les adresses AD d'un réseau programmable (PLA) 11. Pour cela, il comporte deux sorties 17 et 18 connectées à l'une ou à l'autre des deux régions du décodeur d'adresses de la mémoire.

La programmation de la cellule est réalisée par son entrée 12. Un réseau programmable PLA 11 sert à établir les niveaux de programmation. Son entrée de commande 31 est protégée par un fusible 30. Une fois le fusible claqué, la reprogrammation de la cellule 13 est impossible.

A la figure 3, le chronogramme indique l'état des deux bus d'accès 16 et 17. On constate qu'ils sont exclusivement actifs.

A la figure 4, on a représenté une partie du dessin de la mémoire. Un carré de trois cellules de large ou quatre cellules de haut est réservé à la constitution

pour permettre de sauvegarder la régularité du dessin. Le couple 24 de cellules 22 et 23 permet de prévoir la programmation selon l'invention.

5

Revendications

1. Circuit intégré comportant une mémoire qui comprend deux régions d'adresses sélectionnables, caractérisé en ce qu'il comprend en outre deux cellules mémoires (1, 2) programmées, un décodeur d'adresse de la mémoire, les cellules étant lues lors de l'adressage de la mémoire, le signal lu permettant de commander le décodeur (15) de manière à obtenir la sélection de l'une des régions d'adresse ou de l'autre, selon l'état de ces cellules.

10

15

2. Circuit intégré selon la revendication 1, caractérisé en ce qu'il comprend un circuit d'écriture (3) des cellules mémoires et un circuit de sélection des cellules (7), permettant de programmer ces cellules, ces cellules étant lues en permanence lors de l'adressage de la mémoire.

20

25

3. Circuit intégré selon la revendication 1 ou 2, caractérisé en ce que la mémoire (20) est de type EPROM et en ce que les cellules sont constituées par deux transistors à grilles isolées de cette mémoire, une électrode principale de ces deux transistors étant reliée via un amplificateur à une entrée d'une porte ET (6), le signal de sortie de la porte étant utilisé par le décodage des adresses de la mémoire.

30

35

40

45

50

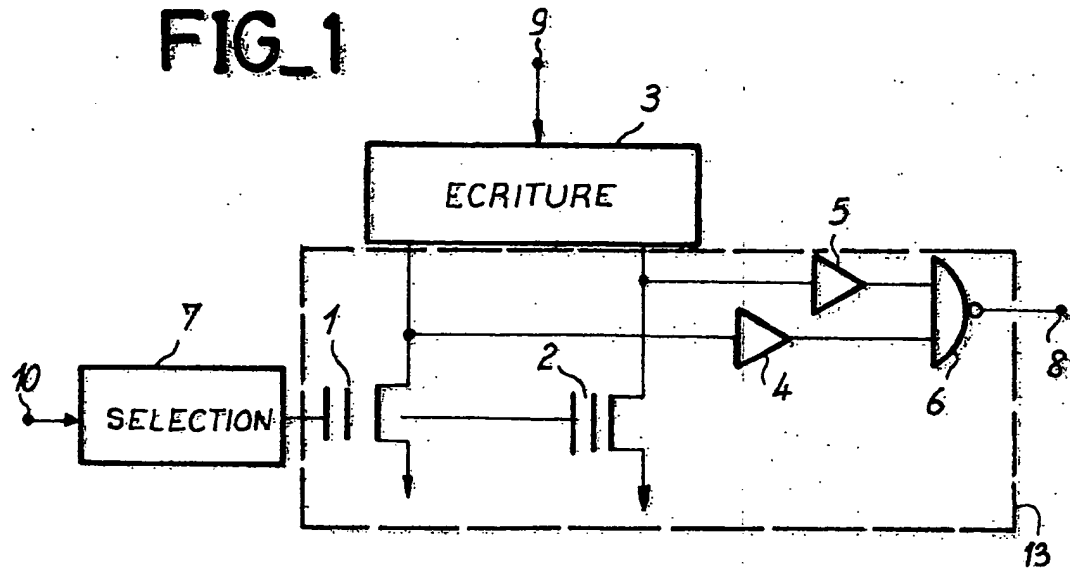
55

60

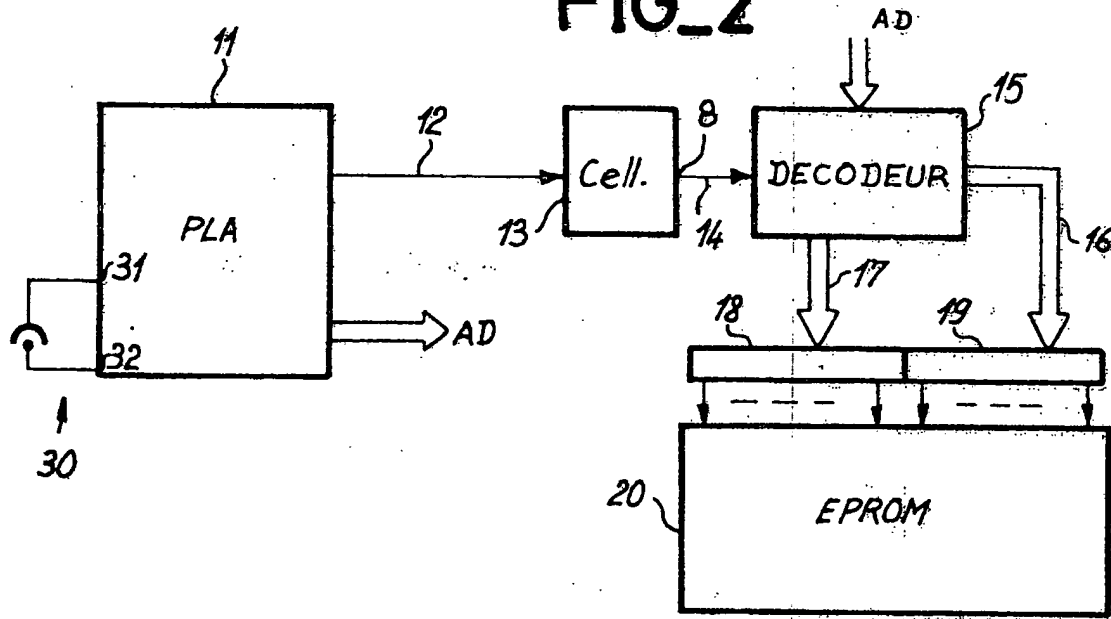
65

3

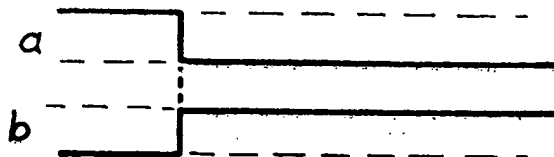
FIG_1



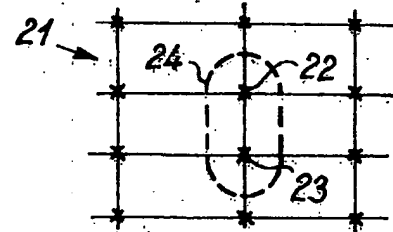
FIG_2



FIG_3



FIG_4





EP 87 40 1435

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.4)
A	US-A-4 521 853 (GUTTAG) * Figure 1; colonne 3, ligne 29 - colonne 4, ligne 26 *	1-3	G 06 F 12/14

A	EP-A-0 136 155 (FUJITSU) * Figures 1,3A,3B; page 3, ligne 22 - page 5, ligne 8; page 5, lignes 17-19 *	1,3	

A	US-A-3 986 169 (KOBAYASHI et al.) * Figures 2,6; colonne 3, lignes 9-22; colonne 4, ligne 10 - colonne 5, ligne 30 *	1	

			DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4)
			G 06 F 12/14 G 06 F 1/00
Le présent rapport de recherche a été établi pour toutes les revendications			
Lieu de la recherche LA HAYE		Date d'achèvement de la recherche 02-10-1987	Examineur LEDROUT P.
CATEGORIE DES DOCUMENTS CITES			
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	